9. Фулфер М. Искусство чтения по лицу / М. Фулфер. – Минск : Попурри, 2004. – 176 с.

10. Хигир Б.Ю. Физиогномика / Б.Ю. Хигир. – М. : Астрель; АСТ; Хранитель, 2007. – 637 с.

11. Шварц Т. Судьба на ладони. Хиромантия / Т. Шварц. – Санкт-Петербург : ПИТЕР, 208. – 144 с.

12. Кестлер Ю. Полный курс хиромантии / Ю. Кестлер. – М. : Из-во Молодая гвардия, 1911. – 80 с.

УДК 341.1

НЕПРАВОМЕРНОЕ ПРИМЕНЕНИЕ КИБЕРСИЛЫ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ГЛОБАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Игорь КАМИНСКИЙ,
аспирант кафедры международного права и международных отношений
Национального университета «Одесская юридическая академия»

Summary

The article is dedicated to the analysis of illegal use of cyber force and the effect of such use on global cyber security. Special attention was focused on the fact that illegal use of cyber force keeps one of the key spots among all threats to global cyber security. Owing to the non-coverage of notion "cyber force" by "force" category under the UN Charter, author argues that such use does not violate Article 2 (4). However, such use was proposed to consider as violation of principle of non-intervention in domestic affairs of other states. It was determined that international community should concentrate on development of measures to counteract illegal use of cyber force for the purpose of ensuring global cyber security.

Key words: international law, non-armed force, cyber force, global cyber security.

Аннотация

Статья посвящена исследованию неправомерного применения киберсилы и влияния, которое оказывает такое применение на обеспечение глобальной кибербезопасности. Акцентируется внимание на том, что среди всех угроз глобальной кибербезопасности одно из ключевых мест занимает неправомерное применение киберсилы. Поскольку понятие «киберсила» не может входить в категорию «сила» по Уставу ООН, обосновано, что такое применение не может нарушать ч. 4 ст. 2. Однако предлагается рассматривать такое применение как нарушение принципа невмешательства во внутренние дела других государств. Установлено, что с целью обеспечения глобальной кибербезопасности международному сообществу необходимо сосредоточить усилия на разработке мер противодействия неправомерному применению киберсилы.

Ключевые слова: международное право, невооруженная сила, киберсила, глобальная кибербезопасность.

Постановка проблемы. Определяющей особенностью эволюции человечества на протяжении последних десятилетий является развитие цифровой сферы. Информационно-цифровая сфера определяет уровень развитости не только отдельных стран и регионов, но и всего мирового сообщества. Государства переносят в киберсферу управление своей инфраструктурой (газопроводами, водоснабжением, электросетями и т.п.), в том числе – отраслью безопасности и обороны. В последние годы киберпространство во все большей степени рассматривается всеми государствами мира как один из важнейших приоритетов безопасности, поскольку все очевиднее становится милитаризация киберпространства. Как следствие, необходимость противодействовать угрозам, приходящим из киберпространства, вызвала выделение специфической сферы как национальной, так и глобальной безопасности – кибербезопасности.

О необходимости международно-правового обеспечения глобальной кибербезопасности свидетельствует серия резолюций Генассамблеи ООН, в которых последняя подчеркнула, что «распространение и использование информационных технологий и средств затрагивает интересы всего международного сообщества» [1], что «преступное использование информационных технологий может иметь серьезные последствия для всех государств» [2] и что эти технологии «потенциально могут быть использованы в целях, несовместимых из задачами обеспечения международной стабильности и безопасности» [3].

Состояние исследования. Среди авторов, занимавшихся вопросом толкования кибербезопасности, разработкой международно-правовых мер ее обеспечения, можно выделить работы

таких ученых: Р. Бакена, Н. Мельцера, М. О'Коннэл, Д. Холлиса, Н. Цагурияса и других. При этом без внимания исследователей остался анализ места и особенностей неправомерного применения киберсилы в призме обеспечения глобальной кибербезопасности.

Целью статьи является установление роли неправомерного применения киберсилы в системе обеспечения глобальной кибербезопасности путем определения особенностей такого применения, исследования имеющихся международно-правовых барьеров неправомерного применения киберсилы и определения их эффективности.

Изложение основного материала. Международный союз электросвязи (МСЭ) определяет кибербезопасность как совокупность средств, политики, концепций, гарантий и руководящих принципов безопасности, подходов к управлению рисками, действий, учений, передовой практики, технологий, которые могут быть использованы для защиты киберсреды, киберустройства и активов пользователей [4]. В отличие от такого сущностного подхода МСЭ, украинский законодатель применил функциональную модель определения кибербезопасности. Так, в Стратегии кибербезопасности Украины она определяется как состояние защищенности жизненно важных интересов человека и гражданина, общества и государства в киберпространстве, которое достигается комплексным применением совокупности правовых, организационных, информационных мер [5]. В рамках этого исследования о кибербезопасности будет идти речь в последнем понимании.

Как демонстрирует практика, основными угрозами глобальной кибербезопасности являются киберпреступность, хакерские атаки, кибершпионаж. Представляется, что особую опасность несет неправомерное применение киберсилы, разработка международно-правовых механизмов борьбы с актами которого придается значительно меньше внимания, чем, например, аналогичным мерам, связанным с киберпреступностью.

Необходимо особо заметить, что неправомерное применение киберсилы и киберпреступность – это две разнородные категории. Ключевым в таком разграничении является личность правонарушителя, ведь киберсила применяется государством или государственными акторами, в то время как субъектами киберпреступлений являются частные лица. При этом в первом случае подлежит применению публичное международное право, а в случае киберпреступности применяется национальное уголовное право соответствующих государств. В контексте этого, например, Конвенцию Совета Европы о киберпреступности следует рассматривать как инструмент сотрудничества государств относительно противодействия соответствующим актам на своих территориях, но она не может применяться к случаям неправомерного применения киберсилы между государствами.

В свою очередь, под неправомерным применением киберсилы следует понимать нарушающий международное право акт одного субъекта международного права против другого субъекта международного права, который состоит во введении, передаче, повреждении, уничтожении, ухудшении, замене либо скрытии компьютерных данных, который осуществлен с использованием компьютерных или связанных с ними сетей или систем и способен нанести вредные последствия потерпевшему субъекту.

Количество и частота подобных случаев особо увеличилась в последние годы. Так, в 2010 г. иранский ядерный центр в Натанзе был поражен компьютерным «червем» *Stuxnet*, что привело к потере контроля над его центрифугами [6].

Через несколько месяцев так называемые атаки относительно «отказа в обслуживании» *(Denial of service attack)* привели к отсутствию Интернет-связи в Бирме, что имело масштабное значение для проведения в этой стране выборов. Хотя в организации этого нападения обвинялась военная хунта Мьянмы, исполнителей кибератаки установлено не было [7].

Эффективное обеспечение глобальной кибербезопасности возможно только путем международного сотрудничества и единым подходом к вопросу квалификации актов неправомерного применения киберсилы. В связи с этим возникает вопрос, какие, собственно, международно-правовые нормы нарушают эти акты? Представляется, что наиболее очевидным, но не общепринятым, является нарушение принципа невмешательства во внутренние дела другого государства.

Необходимо заметить, что некоторые ученые или не уделяют внимания возможности нарушения принципа невмешательства при кибератаках, или считают, что вмешательство в киберпространство другого государства не может рассматриваться как противоправное вмешательство по данному принципу. Например, как объясняет С. Кенак, «с трудом верится, что вмешательство одного государства с помощью нематериальных средств, таких как радиация или электричество, создает *per se* правонарушения против другого государства» [8, с. 288].

Р. Бакен придерживается противоположной позиции. На его взгляд, концепция государственного суверенитета распространяется не только на физическую территорию государства, а выходит за рамки понятия территориального контроля. Ученый это обосновывает тем, что государственный суверенитет защищает от внешних вмешательств право государства осуществлять определенную политику и принимать решения относительно внутренних и внешних вопросов [9, с. 223].

Такое широкое понимание концепции государственного суверенитета нашло текстуальную поддержку в материалах Международного Суда ООН. В решении по делу о военной и полувоенной деятельности в и против Никарагуа (Никарагуа против США) Суд определил как обычный статус принципа невмешательства, так и его объем: «Запрещенное вмешательство должно ... касаться вопросов, которые каждое государство, по принципу государственного суверенитета, свободно решает. Одними из таких вопросов является выбор политической, экономической, социальной и культурной систем и формирования внешней политики. Вмешательство является неправомерным, если оно проводится методами принуждения в отношении таких вопросов, решение которых должно оставаться свободным» [10].

Исходя из директив, М. Джамнеджад и М. Вуд отмечают, что «сутью вмешательства является принуждение, акты которого должны обладать достаточной величиной, чтобы квалифи-

цироваться, собственно, как принудительные и таким образом подпадать под действие принципа невмешательства» [11, с. 345]. В связи с этим представляется, что удачным индикатором «достаточной величины» будет то, предназначен ли акт для того, чтобы принудить потерпевшее государство изменить свою политику.

Кроме того, как подчеркивает Л. Дамрош, важным в этом контексте является то, что принуждение должно применяться относительно вопросов, которые потерпевшее государство вправе само свободно определять, словами Международного Суда, «вопросы, решение которых должно оставаться свободным» [12, с. 2].

На примере кибератак в Эстонии в 2007 г. следует установить, имело ли целью это применение киберсилы принудить эстонское правительство изменить свою политику? В конце апреля 2007 г. эстонское правительство приняло решение о переносе места расположения монумента бронзового солдата, мотивируя это тем, что этот памятник напоминал о советских военных и был символом иностранной оккупации Эстонии. Учитывая большое количество русскоязычного населения в этой стране, такое решение спровоцировало многодневные массовые беспорядки в Таллине, которые сопровождались многочисленными кибератаками как против государственных учреждений, так и частных компаний. Поскольку в то время Эстония считалась «самой информатизированной европейской страной», трехнедельные кибератаки значительно подорвали нормальное функционирование нескольких сфер ее деятельности. Как отметил спикер эстонского парламента, «когда я смотрю на ядерный взрыв и взрыв, имевший место в нашей стране, то вижу одно и то же ... Кибервойна вроде ядерной радиации не приводит к кровотечениям, однако она может разрушить что угодно» [13].

Учитывая тяжкость и продолжительность указанных кибератак, следует, что они достигли такого уровня, что оказали влияние на эстонское правительство с целью принудить его изменить свою политику по локализации монумента.

Другим аспектом является то, касалось ли принуждение вопроса, который правительство вправе само свободно решать. Как представляется, решение о размещении (перемещении) памятников разной степени важности является свободным выбором любого правительства. Другими словами, это решение находится в пределах суверенной сферы национальных правительств и защищается принципом невмешательства.

Основываясь на анализе инцидента в Эстонии, можно сделать вывод, что неправомерное применение киберсилы представляет собой нарушение государственного суверенитета и, соответственно, принципа невмешательства во внутренние дела другого государства.

Несмотря на то, что обыденная интерпретация категории «сила» может быть осуществлена достаточно широко и включать в себя как вооруженные, так и невооруженное формы принуждения, значительная группа ученых сегодня рассматривают понятие «сила» в ч. 4 ст. 2 Устава ООН как синоним к «вооруженной» или «военной» силе.

Д. Холлис считает, что понятие «сила» в значении Устава ООН не распространяется на атаки, совершенные в киберпространстве. По его мнению, природа кибератак, широкий спектр возможных последствий, проблемы с атрибуцией и негосударственными акторами исключают применения ч. 4 ст. 2 [14, с. 1023].

По мнению М. О'Коннел, попытки ученых использовать критерии применения вооруженной силы в случае самообороны в условиях кибератак являются тяжелой или вообще невыполнимой задачей. Исследовательница считает, что в этом случае отсутствуют как соответствующие средства, так и соответствующие последствия, необходимые для применения ст. 51 Устава ООН. Используя дело Никарагуа против США, М. О'Коннел акцентирует внимание на важности критерия «масштабов и последствий», который среди других был применен Судом для определения, могут ли специфические действия классифицироваться как вооруженное нападение [15, с. 5–7].

Уязвимость государств к киберугрозам, в особенности к неправомерному применению киберсилы, обусловлена также трудностями, связанными с точной атрибуцией указанных деяний субъектам, их совершившим. Н. Цагуриас выделяет три основные характеристики киберпространства, которые делают процесс атрибуции в нем очень сложным. Первой является анонимность, что позволяет нападающему скрыть свою идентичность; второй является возможность осуществления многоуровневых кибератак с компьютеров, находящихся в разных юрисдикциях; третьей – скорость, с которой неправомерное применение киберсилы может материализоваться. Кроме того, ключевой сложностью, по мнению Н. Цагуриаса, является не столько обратное отслеживание источника атаки, например, компьютера, как идентификация лица, которое им управляло и лица, руководившего всей атакой [16, с. 233]. Например, в DoS-атаки против Эстонии были вовлечены около 85 тыс. сломанных компьютеров с 178 стран [17], что сделало даже выборочную идентификацию физических исполнителей и организаторов очень сложным процессом.

Как видно, обеспечение глобальной кибербезопасности обязательно должно включать меры по противодействию неправомерному применению киберсилы, что рассматривается как один из ее подрывных элементов. Однако на сегодняшнем этапе развития правоохранительных механизмов ООН вектор обеспечения законности в киберпространстве не соответствует многочисленным вызовам, которые имеют место в этой сфере. Это подтверждает как небольшое количество резолюций, посвященных нормированию поведения государств в виртуальной среде, так и отсутствие стремления ввести, собственно, такое регламентирование.

Представляется, что международно-правовые меры по противодействию неправомерному применению киберсилы должны разделятся на нормативные и институциональные. Так, первоочередной задачей является принятие общеобязательного международно-правового документа, который бы устанавливал формальный запрет прибегать к неправомерному применению киберсилы; предоставлял нормативное определение, собственно, такого применения; содержал перечень признаков актов, составляющих неправомерное применение киберсилы; закладывал основы международно-правового противодействия такому применению и т.п.

Очевидно, основным звеном международно-институционального механизма противодействия актам неправомерного применения киберсилы должен быть Совет Безопасности ООН, учитывая его роль в обеспечении международного мира и безопасности. По Уставу ООН, если Совет Безопасности определит любую угрозу миру или нарушения мира, например неправомерное применение киберсилы, он может принять такие меры, которые будут необходимы для поддержания или восстановления международного мира и безопасности. Такие меры могут быть ограничены предоставлением рекомендаций (ст. 39) или призванием заинтересованных сторон выполнять нормативные обязательства (ст. 40), однако могут также включать невооруженное принуждение (ст. 41) [18].

Однако если Совбез придет к выводу, что меры, которые не предусматривают применение вооруженной силы, есть или будут недостаточными, он «имеет полномочия принять такие действия воздушными, морскими или сухопутными силами, которые окажутся необходимыми для поддержания или восстановления международного мира и безопасности» (ст. 42). В этом контексте в доктрине поднимается вопрос, если атака имеет место в киберпространстве, то не запрещает ли Устав ООН Совету Безопасности принимать соответствующие меры в других видах пространства, чем воздушный, морской или сухопутный? Стоит согласиться с Н. Мельцером, который считает, что целью ст. 42 Устава было не ограничение средств принуждения, доступных Совету Безопасности, а их расширение до всех видов военных актов, которые были в наличии ведущих государств на момент разработки Устава. То есть если смотреть на ст. 42 из телеологической перспективы, можно уверенно утверждать, что она не имеет целью «отнять» у Совета Безопасности полномочия применять силу в ответ на угрозы, которые имеют место в киберпространстве [19, с. 19].

Кроме того, как отметил Международный уголовный трибунал по бывшей Югославии, категория «угроза миру» является в большей степени политической категорией, что предоставляет Совету Безопасности широкую свободу действий [20]. То есть как вопрос права определение «угрозы миру» не предусматривает ни международно-противоправного деяния, ни угрозы или применения силы или наличия вооруженного нападения в значении Устава ООН. Таким образом, Совет Безопасности имеет право принимать меры, включающие вооруженную силу против угроз, которые не порождают права на самооборону, в том числе в случаях неправомерного применения киберсилы.

С другой стороны, свобода действий Совбеза в ситуациях определения, является ли неправомерное применение киберсилы угрозой миру, небезгранична. Ведь Совет Безопасности обязан действовать в соответствии как с целями и принципами Устава, так и с «принципами справедливости и международного права» [18].

Выводы. Итак, глобальная кибербезопасность является одним из факторов, влияющих на стабильность международных отношений. В то же время киберпреступность, хакерские атаки, неправомерное применение киберсилы подрывают эту стабильность. Последнее характеризуется особенно разрушающим воздействием, что позволяет рассматривать неправомерное применение киберсилы как масштабный барьер надлежащего обеспечения глобальной кибербезопасности.

Такой вывод подтверждается тем, что неправомерное применение киберсилы нарушает, как минимум, один основной принцип международного права – принцип невмешательства во внутренние дела других государств. Именно поэтому надлежащее обеспечение глобальной кибербезопасности обязательно должно включать меры по противодействию неправомерному применению киберсилы.

Установлено, что нормативной составляющей таких мер должно стать принятие международно-правового документа по вопросам неправомерного применения киберсилы. Кроме его основной цели (признание международным сообществом недопустимости прибегать к подобным актам), документ должен устанавливать предметные рамки такого применения, основы международного сотрудничества по противодействию актам неправомерного применения киберсилы, определять основы международно-институционального контроля и надзора за подобными актами и т.п.

Доказано, что центральное место в институциональном механизме противодействия актам неправомерного применения киберсилы должно отводиться Совету Безопасности ООН – ключевому гаранту обеспечения международного мира и безопасности. Ведь если последний признает акт неправомерного применения киберсилы как угрозу миру или нарушение мира, то он будет обладать всем спектром средств (в том числе, военных) для пресечения подобного международно-противоправного деяния.

Список использованной литературы:

1. General Assembly Resolution A/RES/55/28 (2000) [Электронный ресурс]. – Режим доступа : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/561/07/PDF/N0056107.pdf?OpenElement..

2. General Assembly Resolution A/RES/55/63 (2001) [Электронный ресурс]. – Режим доступа : https://ccdcoe.org/sites/default/files/documents/UN-001204-CriminalMisuseIT.pdf.

3. General Assembly Resolution A/RES/58/32 (2003) [Электронный ресурс]. – Режим доступа : https://ccdcoe.org/sites/default/files/documents/UN-031208-ITIS_0.pdf.

4. Cybersecurity [Электронный ресурс]. – Режим доступа : http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.

5. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про стратегію кібербезпеки України"» [Электронный ресурс]. – Режим доступа : http://zakon3.rada.gov.ua/laws/show/96/2016.

6. Stuxnet worm 'targeted high-value Iranian assets' – BBC News [Электронный ресурс]. – Режим доступа : http://www.bbc.com/news/technology-11388018.

7. Burma hit by massive net attack ahead of election – BBC News [Электронный ресурс]. – Режим доступа : http://www.bbc.com/news/technology-11693214.

8. Kanuck S. Recent Development: Information Warfare: New Challenges

for Public International Law // Harvard International Law Journal. – 1996. – Vol. 37. – P. 272–292.

9. Buchan R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? // Journal of Conflict and Security Law. – 2012. – Vol. 17. – № 2. – P. 211–227.

10. Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) // I.C.J. Rep. – 1986. – Paragraph 205.

11. Jamnejad M. and Wood M. The Principle of Non-Intervention // Leiden Journal of International Law. – 2009. – Vol. 22. – P. 345–381.

12. Damrosch L. Politics across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs // American Journal of International Law. – 1989. – Vol. 83. – P. 1–50.

13. Hackers Take Down the Most Wired Country in Europe – Wired Magazine [Электронный ресурс]. – Режим доступа : http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

14. Hollis D. Why States Need an International Law for Information Operations // Lewis and Clark Law Review. – 2007. – Vol. 11. – P. 1023–1061.

15. O'Connell M. Cyber Security and International Law // International Law Meeting Summary. – 2012. – 12 p.

16. Tsagourias N. Cyber Attacks, Self-Defence and the Problem of Attribution // Journal of Conflict and Security Law. – 2012. – Vol. 17 № 2. – P. 229–244.

17. Tikk E., Kaska K. and Vihul L. International Cyber Incidents : Legal Considerations [Электронный ресурс]. – Режим доступа : https://ccdcoe.org/publications/books/legalconsiderations.pdf.

18. Charter of the United Nations and Statute of the International Court of Justice [Электронный ресурс]. – Режим доступа : https://treaties.un.org/doc/publication/ctc/uncharter.pdf.

19. Melzer N. Cyberwarfare and International Law [Электронный ресурс]. – Режим доступа : http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

20. Prosecutor v. Dusko Tadić (1995). Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction. – Paragraph 29 [Электронный ресурс]. – Режим доступа : http://www.icty.org/x/cases/tadic/acdec/en/51002.htm.

УДК 340.1

ТЕОРЕТИЧЕСКАЯ МОДЕЛЬ ПОСТРОЕНИЯ МУНИЦИПАЛЬНЫХ ОРГАНОВ ПРАВОПОРЯДКА В УКРАИНЕ

Наталия КАПИТОНОВА,
соискатель кафедры теории государства и права
Национальной академии внутренних дел

Summary

The doctrinal positions of researchers in the context of models for the construction and functioning of municipal law enforcement bodies are investigated, the determinants of influence on the theoretical model of the construction of the municipal police in Ukraine are disclosed, a theoretical model for the construction of the municipal police of Ukraine with the definition of the structural and functional characteristics

Key words: law enforcement body, law and order body, municipal law enforcement body, municipal police

Аннотация

Исследованы доктринальные позиции исследователей в контексте моделей построения и функционирования муниципальных органов правопорядка, раскрыты детерминанты влияния на теоретическую модель построения муниципальной полиции в Украине, предложена теоретическая модель построения муниципальной полиции Украины с определением структурно-функциональной характеристики

Ключевые слова: правоохранительный орган, орган правопорядка, муниципальный орган правопорядка, муниципальная полиция.

Постановка проблемы. Опыт многих стран мира показывает, что формирование специальных органов правопорядка в структуре исполнительных органов местного самоуправления положительно влияет на рост эффективности обеспечения общественного порядка. Сейчас обеспечение общественного порядка осуществляется, прежде всего, рядом правоохранительных органов. Беря во внимание право территориальной общины самостоятельно решать вопросы охраны порядка на территории органа местного самоуправления, все больше органов местного самоуправления инициируют создание собственных муниципальных органов.

Актуальность темы. Эффективность выполнения возложенных на муниципальные органы правопорядка функций детерминирует необходимость поиска наиболее оптимальной организационно-функциональной структуры такого подразделения. Однако и по сей день взгляды на структуру данного органа правопорядка являются неунифицированными в научных кругах.

Состояние исследования. Среди отечественных и зарубежных исследователей отдельные аспекты затронутой проблематики рассматривались такими исследователями, как: В. Басс, Е. Белозеров, Т. Гудзь, С. Гусарев, В. Дубовик, А. Завальный, И. Зозуля, А. Каминский, Я. Когут , А. Кучук, Н. Лазнюк, П. Онопенко, А. Онуприенко, В. Орлов, Т. Пикуля, А. Поклонский, А. Проневич, К. Сесемко, О. Тюрина, Н. Харченко, Р. Шай.

Целью статьи является исследование состояния и перспектив структурно-функциональной модели построения муниципальных органов правопорядка в Украине.

Изложение основного материала. Становление гражданского общества в Украине невозможно без децентрализации публичной власти и реального развития местного самоуправления как одного из наиболее действенных механизмов согласования интересов государства, территориальной общины и отдельной личности.

Несмотря на ратификацию Европейской хартии местного самоуправления, принятие законов Украины «О местном самоуправлении в Украине» и «О местных государственных администрациях», а также ряда других нормативно-правовых актов по вопро-